Threat hunting case study: Medusa ransomware

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 13:03:21 UTC

The **Medusa** ransomware-as-a-service (RaaS) group appeared in 2021 and is one of the most active RaaS programs. The group and its affiliates use the Medusa ransomware strain during attacks, encrypting infected files with the .medusa extension and deploying a ransom note on the victim's hosts. The group mostly targets small and medium-sized entities with revenues ranging from US $5 million to US $50 million. The group practices double extortion, where sensitive data is first discreetly extracted from systems that have been compromised. If an organization doesn't pay a ransom for the decryption key, **Medusa** threatens to release data on its data leak blog, which it launched in 2023.

The group has appeared to benefit from law enforcement actions against other top ransomware operations. Its attacks rose significantly in March 2024 at about the same time the ALPHV aka BlackCat RaaS terminated its operations following law enforcement disruption and the disruption of the LockBit RaaS. The increased law enforcement scrutiny likely forced many affiliates to shift to other RaaS programs, and **Medusa's** lucrative offers possibly attracted them. Just prior to the rise in the number of new victims, **Medusa** announced an intake of new affiliates and offered higher shares of ransoms ranging from 70% to 90%, 24/7 support and the availability of several support "teams" within the group to aid in facilitating attacks.

The RaaS has attracted multiple experienced actors in the past and still cooperates with reputable, capable threat actors, making it a significant threat. According to an advisory from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), **Medusa** has likely impacted more than 300 organizations as of February 2025. Since the beginning of this year through May 11, 2025, Intel 471 has recorded 90 entities that have purportedly been infected by **Medusa** or its affiliates, putting the group in the top 10 most active for 2025.

The program is led by a threat actor going by the monikers **MDS** and **boss** who assigns strict roles to each member of the group. The group partners with initial access broker (IAB) affiliates who provide access to pools of potential victims. CISA says IAB affiliates can receive payments of US $100 to US $1 million to work exclusively for **Medusa**. These IABs gain access to organizations by executing phishing campaigns aimed at collecting login credentials and exploiting unpatched software vulnerabilities. The group mainly focuses on compromising Windows-based hosts but also uses strains to target VMware ESXi hypervisors and Linux-based hosts. Once inside a network, its tactics, techniques and procedures (TTPs) often rely on using living-off-the-land (LOTL) techniques and native Windows tools including PowerShell and Windows Management Instrumentation (WMI).

One of **Medusa's** documented TTPs involves bypassing user account control (UAC), which is a security feature that's aimed at preventing malware from running with administrator privileges on Windows machines. Windows users typically sign in with a standard user account. If an action requires administrative or elevated privileges, UAC will prompt the user for consent. These privileges are also called integrity levels. For example, an application with a high integrity level might be able to modify system data, while lower integrity ones would be forbidden. If a UAC prompt is approved, the action will run with the highest available privilege. Despite

addressing a security concern, Microsoft doesn't consider UAC a security boundary, and attackers have refined various ways for skirting it.

One of the methods **Medusa** uses to bypass UAC is via the Component Object Model (COM), an interoperability standard created in the 1990s. COM objects are reusable mini-programs that other applications can call on to perform functions such as opening a file, communicating with the registry or managing settings. COM objects have been targeted by malicious actors for a number of years, and research published by Mandiant in June 2019 describes how COM objects can be used by attackers. MITRE's ATT&CK knowledge base covers abuse of COM interfaces as a sub-technique under UAC bypass methods.

Intel 471's HUNTER platform contains a threat hunting package called "UAC Bypass Attempt Via Elevated COM Abuse" to hunt for potential COM object abuse. This content is designed to detect UAC bypass attempts abusing common COM interfaces within the registry key HKLM\Software\Microsoft\Windows NT\CurrentVersion\UAC\COMAutoApprovalList. These COM objects are designed to start at a higher integrity level and can be manipulated to open another process at the same higher level. This specific style of COM manipulation is used not only by **Medusa**, but also other ransomware groups including **BlackMatter**, **LockBit 3.0**, **SubZero** and **Trigona**. This threat hunt content is available for free upon registration of an account in HUNTER's Community Portal here.

Let's walk through a hunt using this query. This query contact is compatible with the following endpoint, detection and response (EDR) and logging aggregation platforms: CarbonBlack Cloud - Investigate, CarbonBlack Response, CrowdStrike, CrowdStrike LogScale, Elastic, Google SecOps, Microsoft Defender, Microsoft Sentinel, Palo Alto Cortex XDR, QRadar Query, SentinelOne, Splunk, Tanium, Tanium Signal and Trend Micro Vision One.

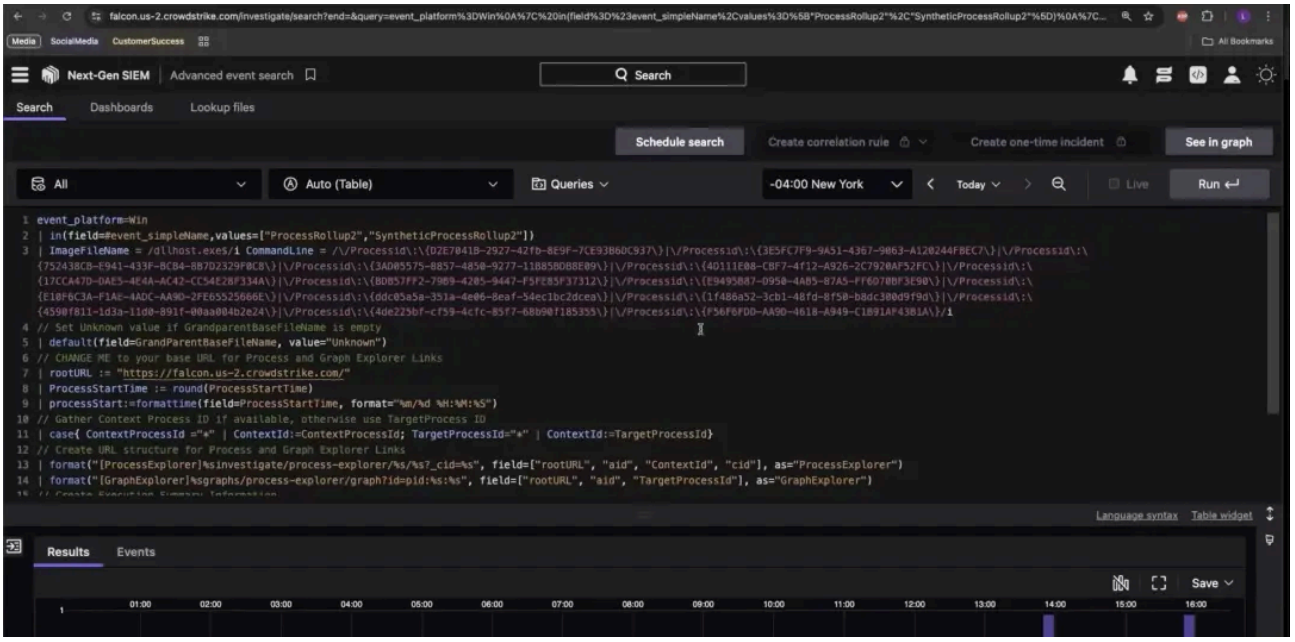
We're looking for COM objects that have a higher integrity level and could be manipulated to open another process at the same higher level. The query focuses on looking for values assigned to those COM objects in the command-line arguments. What follows is a screenshot of the query logic:

QUERY LOGIC

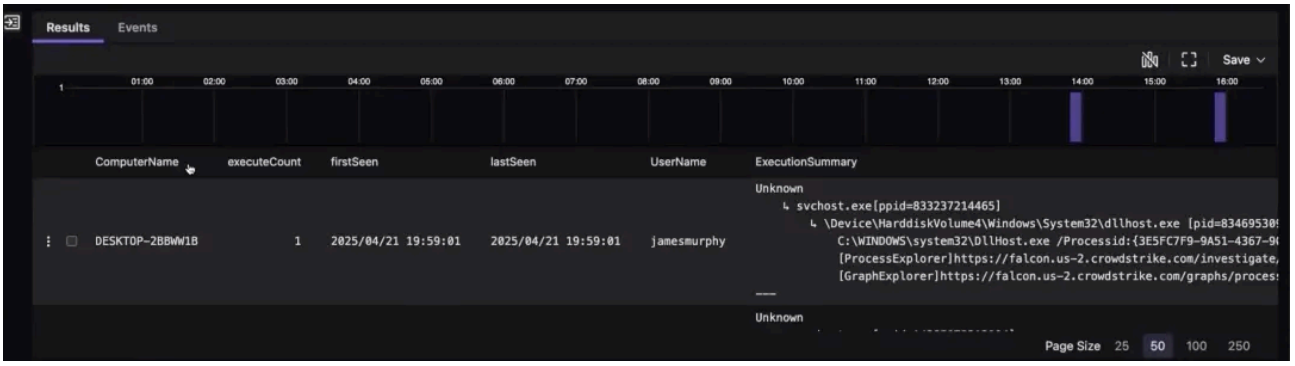
Selection	Field	Value
processPath	process_path	*dllhost.exe
processPath (ANY)	process_cmdline	*/Processid:{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}*
	process_cmdline	*/Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}*
	process_cmdline	*/Processid:{752438CB-E941-433F-BCB4-8B7D2329F0C8}*
	process_cmdline	*/Processid:{3AD05575-8857-4850-9277-11B85BDB8E09}*
	process_cmdline	*/Processid:{4D111E08-CBF7-4f12-A926-2C7920AF52FC}*
	process_cmdline	*/Processid:{17CCA47D-DAE5-4E4A-AC42-CC54E28F334A}*
	process_cmdline	*/Processid:{BDB57FF2-79B9-4205-9447-F5FE85F37312}*
	process_cmdline	*/Processid:{E9495B87-D950-4AB5-87A5-FF6D70BF3E90}*
	process_cmdline	*/Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}*
	process_cmdline	*/Processid:{ddc05a5a-351a-4e06-8eaf-54ec1bc2dcea}*
	process_cmdline	*/Processid:{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}*
	process_cmdline	*/Processid:{4590f811-1d3a-11d0-891f-00aa004b2e24}*
	process_cmdline	*/Processid:{4de225bf-cf59-4cfc-85f7-68b90f185355}*
	process_cmdline	*/Processid:{F56F6FDD-AA9D-4618-A949-C1B91AF43B1A}*
parentProcess	parent_process_path	*dllhost.exe
parentProcess (ANY)	parent_process_cmdline	*/Processid:{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}*
	parent_process_cmdline	*/Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}*
	parent_process_cmdline	*/Processid:{752438CB-E941-433F-BCB4-8B7D2329F0C8}*
	parent_process_cmdline	*/Processid:{3AD05575-8857-4850-9277-11B85BDB8E09}*
	parent_process_cmdline	*/Processid:{4D111E08-CBF7-4f12-A926-2C7920AF52FC}*
	parent_process_cmdline	*/Processid:{17CCA47D-DAE5-4E4A-AC42-CC54E28F334A}*
	parent_process_cmdline	*/Processid:{BDB57FF2-79B9-4205-9447-F5FE85F37312}*
	parent_process_cmdline	*/Processid:{E9495B87-D950-4AB5-87A5-FF6D70BF3E90}*
	parent_process_cmdline	*/Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}*
	parent_process_cmdline	*/Processid:{ddc05a5a-351a-4e06-8eaf-54ec1bc2dcea}*
	parent_process_cmdline	*/Processid:{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}*
	parent_process_cmdline	*/Processid:{4590f811-1d3a-11d0-891f-00aa004b2e24}*
	parent_process_cmdline	*/Processid:{4de225bf-cf59-4cfc-85f7-68b90f185355}*
	parent_process_cmdline	*/Processid:{F56F6FDD-AA9D-4618-A949-C1B91AF43B1A}*
filter	process_path	*werfault.exe

The query logic looks for process paths containing *dllhost.exe and process IDs that are attached to globally unique identifiers (GUIDs). GUIDs are [128-bit identifiers] used to identify a COM interface or software components.

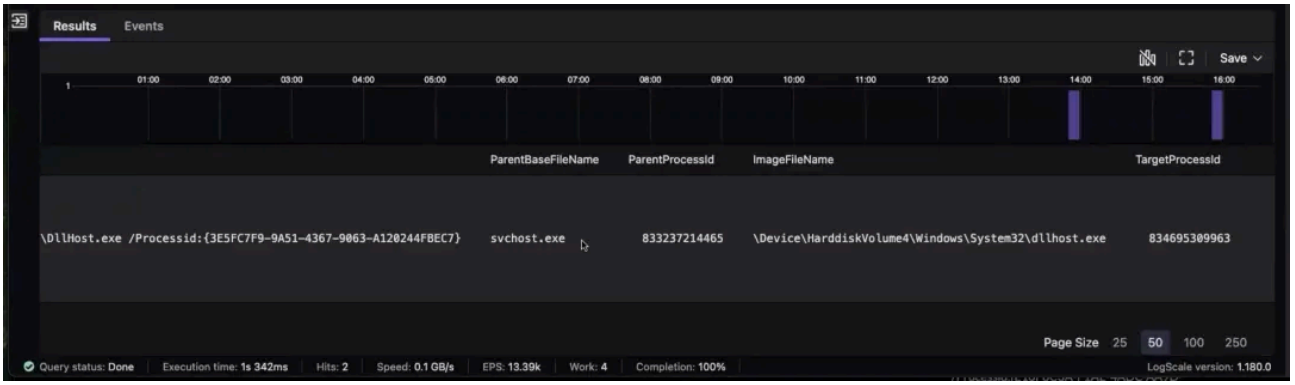
For this demonstration, we will use the query for CrowdStrike's EDR using CrowdStrike's query language. The following screenshot shows part of the query. Visible is the event type that is being searched for, which is a ProcessRollup or a SyntheticProcessRollup. Below that is the ImageFileName, which is dllhost.exe followed by the various ProcessIDs, which contain the GUIDs we are looking for in the command-line argument field.



The query generates one result.



The result shows the affected machine, the username and how many times it has happened. As seen in the screenshot below, it also shows the ParentProcessID and the ImageFileName or child process that was targeted.



This activity is not necessarily malicious but it is suspicious, especially if it cannot be traced to svchost.exe. Perhaps it is business as usual, but at this point, there is some suspicious behavior possibly related to using COM objects to bypass UAC. From here, threat hunters could investigate other activities that occurred around this event such as if the intruders gained privilege escalation or if other processes were spawned.

We hope this tutorial on this UAC bypass technique has been helpful. A video version is available here. Be sure to register for a HUNTER Community Edition account, which contains free sample hunt packages, including the one described in this blog post. Intel 471's HUNTER contains a package of threat hunts that addresses the Medusa ransomware, including queries for behaviors such as:

- Installation (and usage) of malicious tooling
- Privilege escalation via user addition(s) to security groupings
- Manipulation of remote desktop protocol (RDP)-related settings to force a system to be more susceptible

A Community Edition account also will allow for insight into HUNTER's comprehensive library of advanced threat-hunting packages, detailed analyst notes and proactive recommendations. These resources are designed to strengthen your threat-hunting capabilities and keep your organization secure. Happy hunting!
